

				Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII20				Заглавие на документа: Политика за поверителността на децата							
Версия: 1.0		Дата на влизане в сила: 01.01.2025		Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго

История на редакциите				
Номер на редакцията	Дата на редакцията	Промени	Прегледано от	Собственик на процеса

Одобрения			
Име	Длъжност	Дата	Подпис

Правна бележка (авторски права и ограничения за ползване)
(C) 2025 Clarysec LLC. All rights reserved.

Настоящият документ е интелектуална собственост на Clarysec LLC. Никоя част от него не може да бъде копирана, използвана повторно, разпространявана или изменяна за търговски или внедрителски цели без изрично писмено разрешение.

Неупълномощеното използване е строго забранено и може да доведе до правни действия.

За лицензиране се свържете с: info@clarysec.com

Съгласуване със стандарти и регулации

Стандарт / регулация	Клауза / контрол / член	Приложимост	Тип покритие	Коментар
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Документирана информация и оперативен контрол за доказателства относно обработване, свързано с деца
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Мониторинг, несъответствие и коригиращо действие за контролите за поверителност на децата
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Цели, правно основание, съгласие, DPIA и записи на администратора за обработване, свързано с деца
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Договори с обработващи лични данни и отговорности на съвместен администратор за обработване, свързано с деца
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5	Controller	Primary	Задължения към деца, предоставяне на информация и промяна или оттегляне на съгласие
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Задължения относно възражение, достъп, корекция, изтриване, обработване на искания и автоматизирано вземане на решения

ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Ограничения за събиране, обработване, минимизиране, срок за съхранение и унищожаване
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Supporting	Записи за разкриване и обработване на искания за разкриване
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Споразумение с клиента на обработващия лични данни, инструкции, съдействие и записи
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Подкрепа от обработващия лични данни за задълженията към субекта на данни и обработването на разкриване
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Защита на записи и журнализиране за доказателства относно обработване, свързано с деца
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Добросъвестност, прозрачност, ограничаване на целите, минимизиране, ограничаване на съхранението и отчетност
GDPR	Article 6; Article 7; Article 8; Article 9	Controller	Primary	Законосъобразност, условия за съгласие, съгласие на дете и предпазни мерки за специални категории данни
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Прозрачна информация и

				подходящи за деца уведомления
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Права на достъп, коригиране, изтриване, ограничаване, възражение и автоматизирано вземане на решения
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Отговорност на администратора, защита на данните на етапа на проектирането и по подразбиране, съвместни администратори, обработващи лични данни, записи, сигурност, DPIA и задачи на DPO
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Съгласие и избор, прозрачност и участие на физическото лице
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Ограничаване на целите, събирането, минимизирането, използването, съхранението и разкриването
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Отчетност, информационна сигурност и съответствие с изискванията за поверителност
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Полза от PIA, определяне на праг и подготовка за оценка на риска, свързана с деца
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Контроли за съгласие, цел, събиране, минимизиране, съхранение,

				разкриване и участие на субекта
ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Структура на запис за съгласие и потвърждение за съгласие, когато се използват потвърждения за съгласие

1. Обхват

1.1 Тази политика определя задължителните изисквания за поверителност при обработване на PII, включващо деца, услуги, насочени към деца, услуги, до които е вероятно деца да имат достъп, и дейности по обработване, при които PII на деца изисква засилени предпазни мерки.

1.2 Тази политика се прилага за следното:

- 1.2.1 дейности по обработване на PII, включващи деца, в рамките на обхвата на PIMS;
- 1.2.2 уебсайтове, приложения, игри, образователни услуги, онлайн платформи, свързани услуги, клиентски портали, учебни среди, общности и канали за поддръжка, насочени към деца;
- 1.2.3 обработване, при което децата са пряко целеви адресати, вероятни потребители, титуляри на акаунти, учащи, участници, бенефициери или представлявани субекти на данни;
- 1.2.4 оценка на възрастта, родителска отговорност или разрешение от носител на родителска отговорност, удобни за деца уведомления, доказателства за съгласие, оценка на риска за поверителността, критерии за задействане на DPIA, минимизиране, обработване на права, ограничения за обработващи лични данни, споделяне на данни и свързана с безопасността ескалация, включваща PII на деца;
- 1.2.5 контексти на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване.

1.3 Тази политика не заменя следното:

- 1.3.1 PII03 относно инвентара на обработването, правното основание и собствеността върху ROPA;
- 1.3.2 PII04 относно общото управление на уведомленията за поверителност;
- 1.3.3 PII05 относно функционирането на управлението на съгласия и предпочитания;
- 1.3.4 PII06 относно работния поток за искания за упражняване на права на субекти на данни;
- 1.3.5 PII07 относно методологията за оценка на риска за поверителността и DPIA;
- 1.3.6 PII08 относно контролните точки за поверителност още при проектиране и по подразбиране;
- 1.3.7 PII09 относно общите контроли за събиране, използване, разкриване и споделяне;
- 1.3.8 PII10 относно изпълнението на съхранение, изтриване и унищожаване;
- 1.3.9 PII11 относно контроли за точност и качество;
- 1.3.10 PII12 относно управлението на жизнения цикъл на обработващи лични данни, подизпълнители по обработване и трети страни;
- 1.3.11 PII13 относно контролите за международни трансфери;
- 1.3.12 PII14 относно сигурността и контрола на достъпа;
- 1.3.13 PII15 относно обработването на инциденти и нарушения;
- 1.3.14 PII18 относно мониторинга, одита и подобрението;
- 1.3.15 PII21 относно контролите за поверителност при AI и автоматизирано вземане на решения;
- 1.3.16 PII22 относно контролите за поверителност при маркетинг и бисквитки.

2. Цел

2.1 Целта на тази политика е да гарантира, че PII на деца се идентифицира, управлява, минимизира, обяснява, защитава и доказва чрез засилени предпазни мерки за поверителност, подходящи за обработване, насочено към деца и достъпно за деца.

2.2 Тази политика подпомага последователното вземане на решения за обработване, свързано с деца, без да създава отделен регистър на данни за деца, регистър за гарантиране на възрастта, регистър за разрешения от носител на родителска отговорност, табло за безопасност, комитет или неканоничен доказателствен обект.

3. Цели

3.1 Целите на тази политика са да:

- 3.1.1 идентифицира дейностите по обработване, насочени към деца и достъпни за деца, в REG02;
- 3.1.2 дефинира очакванията за оценка на възрастта и разрешение от носител на родителска отговорност, без да предписва специфични за юрисдикция възрастови прагове в самата политика;
- 3.1.3 гарантира, че уведомленията за поверителност, удобни за деца, се поддържат в REG07;
- 3.1.4 гарантира, че доказателствата за съгласие, разрешение от носител на родителска отговорност и оттегляне се поддържат в REG05, когато е приложимо;
- 3.1.5 задейства специфична за деца оценка на риска за поверителността и маршрутизиране за DPIA чрез REG04;
- 3.1.6 гарантира, че исканията за упражняване на права, включващи деца, се обработват чрез REG06;
- 3.1.7 ограничава обработващите лични данни, подизпълнителите по обработване и споделянето на данни, включващи PII на деца, чрез REG08;
- 3.1.8 маршрутизира предполагаеми инциденти с PII на деца, неправомерна употреба, неоторизиран достъп или рискове за PII, свързани с безопасността, чрез REG10 и REG12;
- 3.1.9 поддържа доказателства, годни за одит, за управлението на поверителността на децата чрез REG12.

4. Изявления на политиката

4.1 Идентифициране и разрешаване на обработване, насочено към деца

- 4.1.1 [Controller] Когато се предлага нова или съществено променена услуга, функция, кампания, канал или дейност по обработване, Process Owner / Business Owner трябва да определи дали обработването е насочено към деца, вероятно ще бъде достъпно за деца или по друг начин включва PII на деца, и да запише определянето в REG02.
- 4.1.2 [Controller] Преди събирането на информация, свързана с възрастта, Process Owner / Business Owner трябва да определи минималните данни за оценка на възрастта, необходими за целта на обработването, и да запише метода в REG02.
- 4.1.3 [Controller] Преди да започне обработването на PII на деца, Process Owner / Business Owner трябва да документира целта на обработването, правното основание, конфигурирания възрастов праг за дете, зависимостта от разрешение от носител на родителска отговорност и местоположението на доказателствата в REG02 и REG05, когато се използва съгласие или разрешение.
- 4.1.4 [Joint Controller] Преди PII на деца да се обработва със съвместен администратор, Privacy Lead / PIMS Manager трябва да документира отговорностите за поверителността на децата, отговорността за уведомяване, обработването на права, отговорността за съгласие или разрешение и отговорността за ескалация в REG08.

- 4.1.5 [Processor] Преди обработването на PII на деца за клиент, Process Owner / Business Owner трябва да потвърди, че инструкциите за обработване, свързано с деца, са документирани и отразени в REG08.
- 4.1.6 [Both] Преди обработването на PII на деца да бъде активирано в система или бизнес процес, Privacy Lead / PIMS Manager трябва да потвърди, че индикаторите за данни на деца, отговорните собственици и изискваните доказателствени обекти са записани в REG02 или REG08, според приложимото.

4.2 Прозрачност и уведомявания, удобни за деца

- 4.2.1 [Controller] Преди PII на деца да се събира пряко от дете или родител, Process Owner / Business Owner трябва да гарантира, че е налично уведомяване за поверителност, подходящо за деца, и че то е записано в REG07.
- 4.2.2 [Controller] Когато дадена услуга е проектирана за деца или е вероятно да бъде достъпна за деца, Process Owner / Business Owner трябва да предостави многослойно съдържание на уведомяването, което отделя подходящите за деца обяснения от информацията за родител или настойник, и да запише версията на уведомяването в REG07.
- 4.2.3 [Controller] Когато PII на деца се събира непряко, Process Owner / Business Owner трябва да документира източника, подхода за уведомяване и момента на предоставяне на уведомяването в REG02 и REG07.
- 4.2.4 [Controller] Когато цел на обработване, категория данни, категория получатели, референция за срок на съхранение, механизъм за даване на съгласие или маршрут за упражняване на права при обработване, насочено към деца, се променя, Privacy Lead / PIMS Manager трябва да прегледа и актуализира съответния запис за уведомяване в REG07 преди въвеждането на промяната.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Изключения

- 9.1 [All] Преди отклонение от изискване за поверителност на децата в тази политика, заявяващият Process Owner / Business Owner трябва да подаде обосновка за изключение и доказателства за компенсиращи контроли в REG12.
- 9.2 [Conditional] Когато изключение засяга съгласие на дете, разрешение от носител на родителска отговорност, уведомяване, насочено към деца, профилиране, автоматизирано вземане на решения, резултат от DPIA, разкриване или обработване, свързано с безопасността, Data Protection Officer / Privacy Advisor трябва да прегледа изключението и да запише съвета в REG04 или REG12.
- 9.3 [Conditional] Когато изключение създава или запазва висок остатъчен риск за PII на деца, Top Management трябва да одобри или отхвърли изключението и да запише решението в REG04 и REG12.
- 9.4 [All] Преди одобрено изключение относно поверителността на децата да изтече, Privacy Lead / PIMS Manager трябва да прегледа статуса на приключване, подновяване или коригиращо действие и да запише резултата в REG12.

10. Прилагане на политиката

- 10.1 [All] Когато бъде установено неспазване на тази политика, Privacy Lead / PIMS Manager трябва да запише несъответствието и коригиращото действие в REG12.

- 10.2 [Both] Когато се подозира неоторизирано обработване, разкриване, достъп или използване на PII на деца, Incident Response Coordinator трябва да започне ескалация на инцидент и да запише доказателства в REG10 и REG12.
- 10.3 [Both] Когато обработващ лични данни, подизпълнител по обработване, доставчик или получател при споделяне на данни не изпълни задълженията за поверителност, свързани с деца, Vendor / Procurement Owner трябва да запише действие за отстраняване, ескалация или прекратяване в REG08 и REG12.
- 10.4 [All] Когато възникнат повтарящи се или системни несъответствия относно поверителността на децата, Top Management трябва да прегледа въпроса и да запише управленското действие в REG12.

11. Преглед и поддръжка

- 11.1 [All] Най-малко веднъж годишно Privacy Lead / PIMS Manager трябва да прегледа тази политика за продължаваща пригодност и да запише резултата от прегледа в REG12.
- 11.2 [Conditional] Когато законите, услугите, технологиите, методите за оценка на възрастта, механизмите за даване на съгласие, потребителските пътеки, насочени към деца, или рисковете при обработване се променят съществено, Privacy Lead / PIMS Manager трябва да прегледа засегнатите контроли за поверителност на децата и да запише резултата в REG02, REG04 или REG12.
- 11.3 [Controller] Най-малко веднъж годишно и след съществени промени в интерфейса Process Owner / Business Owner трябва да прегледа съдържанието на уведомленията и съгласието, насочени към деца, и да запише прегледа в REG05 и REG07.
- 11.4 [All] След приключване на коригиращи действия относно поверителността на децата Internal Audit / Compliance Reviewer трябва да провери ефективността и да запише доказателства от проверката в REG12.

12. Свързани политики

- 12.1 PII01 - Политика за Privacy Information Management System
- 12.2 PII02 - Политика за роли, отговорности и отчетност в поверителността
- 12.3 PII03 - Политика за инвентар на обработването на PII и правно основание
- 12.4 PII04 - Политика за уведомления за поверителност и прозрачност
- 12.5 PII05 - Политика за управление на съгласия и предпочитания
- 12.6 PII06 - Политика за управление на правата на субекти на данни
- 12.7 PII07 - Политика за оценка на риска за поверителността и DPIA
- 12.8 PII08 - Политика за поверителност още при проектиране и по подразбиране
- 12.9 PII09 - Политика за събиране, използване, разкриване и споделяне на PII
- 12.10 PII10 - Политика за съхранение, изтриване и унищожаване на PII
- 12.11 PII11 - Политика за точност и качество на PII
- 12.12 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни
- 12.13 PII13 - Политика за международен трансфер на PII
- 12.14 PII14 - Политика за сигурност и контрол на достъпа до PII
- 12.15 PII15 - Политика за управление на инциденти и нарушения с PII
- 12.16 PII17 - Политика за документирана информация и управление на доказателства в PIMS
- 12.17 PII18 - Политика за мониторинг, одит и подобрене в PIMS
- 12.18 PII21 - Политика за поверителност при AI и автоматизирано вземане на решения

12.19 PII22 - Политика за поверителност при маркетинг и бисквитки

13. Референтни стандарти и рамки

- 13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].
- 13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].
- 13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.3.1; 4.3.2; 4.3.5; 4.6.1; 4.8.1; 7.1; 7.2; 7.4].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.3; 4.7.4; 5.7; 6.3; 7.7].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.3; 7.3; 11.3].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.3; 4.6.5; 7.6].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 7.1].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.1; 4.7.2; 4.8.1; 7.7].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.5.4; 4.7.3; 4.7.4; 5.7; 6.3; 7.7].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 7.7].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.6.2; 4.6.4; 4.8.1; 7.5; 7.8; 10.2].
- 13.12 GDPR - Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2). Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.4; 4.4.5; 4.8.1; 8.1].
- 13.13 GDPR - Article 6; Article 7; Article 8; Article 9. Addressed by clauses [4.1.3; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.4.3; 7.4; 11.3].
- 13.14 GDPR - Article 12; Article 13; Article 14. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.3; 11.3].
- 13.15 GDPR - Article 15; Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.3; 4.6.5; 7.6].
- 13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.6.1; 4.6.2; 4.7.3; 4.8.2; 5.3; 6.4; 7.2; 9.2].
- 13.17 ISO/IEC 29100:2020 - Clause 5.1; Clause 5.8; Clause 5.9. Addressed by clauses [4.2.1; 4.2.2; 4.3.1; 4.3.3; 4.5.1; 4.5.2; 4.5.3].
- 13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 4.4.4; 4.4.5; 4.7.1].
- 13.19 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.6.2; 4.6.4; 4.8.1; 4.8.2; 6.1; 8.5; 10.1].
- 13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.4.3; 4.6.1; 4.6.3; 6.4; 7.2; 9.2].
- 13.21 ISO/IEC 29151:2022 - Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 4.5.2; 4.7.1; 7.4].

13.22 ISO/IEC TS 27560:2023 - Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4. Addressed by clauses [4.3.2; 4.3.4; 4.3.5; 7.4].